#3

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of : Docket No. 99-RO-182

Yannick TEGLIA : Group Art Unit: 2185

Serial No. 09/738,893 : Examiner: (not yet assigned)

Filed: December 15, 2000

For: *METHOD FOR THE SECURED TRANSFER OF DATA*

CLAIM FOR PRIORITY UNDER 35 USC §119

Assistant Commissioner for Patents
Washington, D.C. 20231

SIR:

Under the provisions of 35 USC §119, there is filed herewith a certified copy of French Application No. 9915795 filed on December 15, 1999, in accordance with the International Convention for the Protection of Industrial Property, 53 Stat. 1748, under which Applicants hereby claim priority.

Respectfully submitted,

Date: 3/15/01

By: _____
Jon A. Gibbons
Reg. No. 37,333

FLEIT, KAIN, GIBBONS,
GUTMAN & BONGINI P.L.
One Boca Commerce Center
551 Northwest 77th Street, Suite 111
Boca Raton, Florida 33487
Telephone: (561) 989-9812

R E P U B L I Q U E F R A N Ç A I S E

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 17 JAN. 2001

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

CERTIFIED COPY OF PRIORITY DOCUMENT

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS cedex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30
http://www.inpi.fr

DB 267161000
ETABLISSEMENT PUBLIC NATIONAL CREE PAR LA LOI N° 51-444 DU 19 AVRIL 1951

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11354*01

REQUÊTE EN DÉLIVRANCE 1/2

Cet imprimé est à remplir lisiblement à l'encre noire

OB 540 W /260899

Réservé à l'INPI

REMISE DES PIÈCES
DATE 15 DEC 1999
LIEU 54 INPI NANCY

N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 9915795

DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 15 DEC. 1999

Vos références pour ce dossier *(facultatif)* 015344

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

CABINET BALLOT
CONSEILS EN PROP.INDUSTRIELLE
9 RUE CLAUDE CHAPPE
TECHNOPOLE METZ 2000
57070 METZ

Confirmation d'un dépôt par télécopie ☐ N° attribué par l'INPI à la télécopie

2 NATURE DE LA DEMANDE	Cochez l'une des 4 cases suivantes
Demande de brevet	☒
Demande de certificat d'utilité	☐
Demande divisionnaire	☐
Demande de brevet initiale	N° Date / /
ou demande de certificat d'utilité initiale	N° Date / /
Transformation d'une demande de brevet européen *Demande de brevet initiale*	☐ N° Date / /

3 **TITRE DE L'INVENTION** (200 caractères ou espaces maximum)

Procédé de transfert sécurisé de données.

4 **DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE**	Pays ou organisation Date / / N° Pays ou organisation Date / / N° Pays ou organisation Date / / N° ☐ **S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»**
5 **DEMANDEUR**	☐ **S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»**
Nom ou dénomination sociale	STMICROELECTRONICS S.A.
Prénoms	
Forme juridique	S.A.
N° SIREN	
Code APE-NAF	
Adresse — Rue	7 rue Galliéni
Adresse — Code postal et ville	94250 GENTILLY
Pays	FRANCE
Nationalité	Française
N° de téléphone *(facultatif)*	
N° de télécopie *(facultatif)*	
Adresse électronique *(facultatif)*	

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE 2/2

Réservé à l'INPI

REMISE DES PIÈCES
DATE 15 DEC 1999
LIEU 54 INPI NANCY
N° D'ENREGISTREMENT
NATIONAL ATTRIBUÉ PAR L'INPI 9915795

DB 540 W /260899

Vos références pour ce dossier : *(facultatif)*		
6 MANDATAIRE		
Nom		LECLAIRE
Prénom		Jean-Louis
Cabinet ou Société		CABINET BALLOT SCHMIT
N °de pouvoir permanent et/ou de lien contractuel		
Adresse	Rue	18 PLACE DU FORUM
	Code postal et ville	57000 METZ
N° de téléphone *(facultatif)*		03 87 74 81 36
N° de télécopie *(facultatif)*		03 87 36 26 76
Adresse électronique *(facultatif)*		
7 INVENTEUR (S)		
Les inventeurs sont les demandeurs		☐ Oui ☒ Non **Dans ce cas fournir une désignation d'inventeur(s) séparée**
8 RAPPORT DE RECHERCHE		**Uniquement pour une demande de brevet (y compris division et transformation)**
Établissement immédiat ou établissement différé		☒ ☐
Paiement échelonné de la redevance		**Paiement en trois versements, uniquement pour les personnes physiques** ☐ Oui ☐ Non
9 RÉDUCTION DU TAUX DES REDEVANCES		**Uniquement pour les personnes physiques** ☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)* ☐ Requise antérieurement à ce dépôt *(joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence)* :
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		

10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE
(Nom et qualité du signataire)
LECLAIRE Jean-Louis 93.4009

VISA DE LA PRÉFECTURE OU DE L'INPI
CALIGARA

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

DOCUMENT COMPORTANT DES MODIFICATIONS

PAGE(S) DE LA DESCRIPTION OU DES REVENDICATIONS OU PLANCHE(S) DE DESSIN			R.M.*	DATE DE LA CORRESPONDANCE	TAMPON DATEUR DU CORRECTEUR
Modifiée(s)	Supprimée(s)	Ajoutée(s)			
planche 1/1				15/05/00	24 MAI 2000 - 1 F

Un changement apporté à la rédaction des revendications d'origine, sauf si celui-ci découle des dispositions de l'article R.612-36 du code de la Propriété Intellectuelle, est signalé par la mention «R.M.» (revendications modifées).

PROCEDE DE TRANSFERT SECURISE DE DONNEES

L'invention a pour objet un procédé de transfert sécurisé de données dans un circuit programmable. En particulier, l'invention vise à protéger d'une éventuelle inspection les données contenues dans une mémoire lors de leur transfert vers une autre mémoire. L'invention s'applique notamment à tout circuit programmable utilisant des données secrètes.

Les données secrètes sont par exemple des données personnelles identifiant le propriétaire du circuit programmable, des instructions de programme ou bien des clés d'algorithmes de cryptage de données. Les données secrètes sont le plus souvent stockées dans des mémoires mortes du circuit programmable à la fabrication de celui-ci. Des moyens connus sont utilisés pour protéger le contenu des mémoires mortes d'une inspection visuelle. A titre d'exemple, les données peuvent être éparpillées dans la mémoire. Cependant, lorsqu'elles sont utilisées, les données secrètes transitent en clair sur un bus de données qu'il est facile d'espionner.

Une technique d'espionnage classique consiste à mesurer le courant qui circule dans le bus ; il est en effet représentatif de la donnée qui circule dans le bus. Il suffit alors de réaliser K mesures de courant lors de K transits de la même donnée et de moyenner ces K mesures pour éliminer le bruit de la mesure et obtenir la valeur exacte de la donnée. A titre indicatif, il est nécessaire de réaliser environ K = 1000 mesures pour éliminer le bruit et obtenir la valeur exacte de la donnée qui transite sur le bus. Cette technique d'espionnage est connue sous l'expression anglo-saxone "Simple Power Analysis".

De plus, afin de réduire les coûts de fabrication des produits, les données secrètes sont souvent en partie les mêmes pour une famille donnée de circuits

programmables. Aussi, si un espion arrive à lire les données secrètes mémorisées dans un produit, il pourra les utiliser pour toute une famille de produits.

Un but de l'invention est d'améliorer la sécurité des données dans un circuit programmable, et en particulier lors de leur transit sur le bus de données. Pour atteindre ce but, l'invention concerne un procédé de transfert sécurisé de données dans un circuit programmable comprenant une unité de commande, une mémoire morte comprenant des données à transférer, une mémoire inscriptible et un bus de données connecté entre la mémoire morte et la mémoire inscriptible, le bus de données étant commandé par l'unité de commande,

le procédé de transfert étant caractérisé en ce qu'une donnée secrète à transférer de N octets transite octet par octet sur le bus de données, chaque octet transitant une seule fois sur le bus de données, et en ce que les octets sont transférés selon une loi de transfert ayant au moins un paramètre choisi de manière aléatoire par l'unité de commande avant chaque transfert de la donnée secrète.

Le procédé de l'invention consiste donc à transférer les données secrètes sur le bus dans un ordre choisi aléatoirement par l'unité de commande gérant le bus de données, avant chaque transfert de la donnée secrète. Ainsi, avec l'invention, chaque transfert d'une même donnée est effectué dans un ordre différent. Les méthodes d'espionnage couramment utilisées ne suffisent donc plus pour obtenir la valeur exacte d'une donnée secrète transitant sur le bus de données.

Selon un mode préféré de réalisation, le procédé de l'invention utilise une loi de transfert qui est une permutation des éléments de l'ensemble des N octets de la donnée secrète à transférer. De préférence, la permutation est définie par la relation

$$X = (X0 + SENS * PAS * j) \text{ modulo } N,$$

où un premier paramètre PAS, compris entre 0 et N-1, définit le pas de la permutation, où un second paramètre SENS, prenant deux valeurs 1 ou -1, définit le sens de parcours de l'ensemble des N octets de la donnée secrète, où un troisième paramètre X0, compris entre 0 et N-1, définit le point de départ de la permutation, et où un indice courant X, obtenu à partir des premier à troisième paramètres et d'un indice de boucle j variant entre 0 et N-1, indique le poids d'un octet de la donnée secrète à transférer.

Il est à noter que ici, et dans toute la description qui va suivre, l'expression "poids d'un octet" fait référence au rang ou au numéro d'un octet de la donnée secrète. En d'autre terme, une donnée secrète comprend N octets, chaque octet étant repéré par un poids compris entre 0 et N-1, l'octet de poids 0 correspondant aux huit de poids les plus faibles et l'octet de poids N-1 correspondant aux huit bits de poids les plus forts de la donnée secrète.

De préférence le premier et/ou le second et/ou le troisième paramètres sont choisis aléatoirement par l'unité de commande, avant chaque transfert de la donnée secrète. De préférence encore, le premier paramètre de la permutation et le nombre N sont premiers entre eux. Par exemple, le nombre N est un nombre entier premier et le premier paramètre de la permutation est un nombre entier compris entre 1 et N-1.

Selon le mode de réalisation préféré, le procédé de l'invention comprend les étapes suivantes :

E0: Initialisation du procédé et choix des premier à troisième paramètres, l'un au moins des premier à troisième paramètres étant choisi aléatoirement par l'unité de commande, les premier à troisième paramètres étant mémorisés dans un premier registre de l'unité de commande,

E1 : Initialisation de l'indice de boucle et de l'indice courant,

E2 : Répétition N fois des étapes suivantes :

ET1 : lecture, dans la mémoire morte d'un octet de la donnée à transférer, le poids de l'octet lu étant égal à l'indice courant, et mémorisation de l'octet lu dans un second registre de l'unité de commande,

ET2 : écriture dans la mémoire vive, de l'octet contenu dans le second registre,

ET3 : incrémentation de l'indice de boucle et variation de l'indice courant.

Enfin, l'invention a également pour objet un circuit programmable comprenant une unité de commande, une mémoire morte comprenant des données à transférer, une mémoire inscriptible et un bus de données connecté entre la mémoire morte et la mémoire inscriptible, le bus de données étant commandé par l'unité de commande,

le circuit programmable étant caractérisé en ce qu'il comporte en outre un générateur de nombres aléatoires pour fournir au moins un paramètre d'une loi de transfert de données utilisée pour transférer une donnée secrète de N octets de la mémoire morte vers la mémoire vive, les octets de la donnée secrète à transférer transitant octet par octet sur le bus de données, chaque octet transitant une seule fois sur le bus de données, l'au moins un paramètre étant différent à chaque transfert de la donnée secrète.

L'invention sera mieux comprise et d'autres caractéristiques et avantages apparaîtront à la lecture de la description qui va suivre, la description faisant référence au dessin annexé dans lequel :

- la figure 1 est un schéma-bloc d'un circuit programmable mettant en œuvre l'invention,
- la figure 2 est un diagramme d'un algorithme de mise en œuvre d'un transfert sécurisé de données, selon

l'invention.

Le circuit programmable CP de la figure 1 comprend une mémoire morte ROM qui contient une donnée secrète de N octets mémorisés à des adresses s_0 à s_{N-1}, une mémoire vive RAM, une unité de commande UC, un générateur de nombres aléatoires GA et un bus de données DBUS qui relie tous les éléments les uns aux autres.

La mémoire vive RAM est une mémoire inscriptible ou ré-inscriptible, par exemple de type EPROM ou EEPROM. Le générateur de nombres aléatoires GA est un circuit connu qui peut fournir, en réponse à une instruction CO de l'unité de commande UC, des nombres entiers aléatoires compris entre 0 et un nombre entier MAX, par exemple égal à 255. L'unité de commande UC reçoit des instructions contenues dans la mémoire morte ROM et contrôle, entre autre, la mémoire vive RAM et le générateur de nombres aléatoires GA. L'unité de commande UC comprend deux registres RA et RX de un octet chacun.

Bien sûr, le circuit programmable CP comprend également d'autres éléments tels que par exemple des registres de données ou d'instructions, des circuits de calcul arithmétique et logique, des compteurs, des circuits d'horloge ou bien des ports d'entrées et/ou de sortie. Le circuit programmable peut également comprendre plusieurs mémoires vives, plusieurs mémoires mortes et/ou plusieurs générateurs de nombres aléatoires. De plus, tous les éléments du circuit programmable CP peuvent éventuellement communiquer avec un ou plusieurs autres éléments, par l'intermédiaire de bus de commande, de bus de données et/ou de bus d'adresses. Cependant, par souci de simplification, seuls les éléments du circuit programmable CP strictement nécessaires à la compréhension de l'invention ont été représentés sur la figure 1.

Dans un exemple, une donnée secrète de N octets Oct_0 à Oct_{N-1} est mémorisée à des adresses s_0 à s_{N-1} de la

mémoire morte ROM du circuit programmable CP et doit être transférée de la mémoire morte ROM vers la mémoire vive RAM à des adresses d_0 à d_{N-1} pour être utilisée ultérieurement. Dans l'exemple, N est choisi égal à 4.

Le procédé de l'invention consiste à transférer la donnée secrète octet par octet, l'ensemble des N octets étant transféré dans un ordre différent à chaque transfert de la donnée secrète, chaque octet de la donnée secrète étant transféré une et une seule fois lors d'un même transfert de la donnée. Pour cela, le procédé de l'invention utilise une loi de transfert ayant un ou plusieurs paramètres choisis aléatoirement par l'unité de commande avant chaque transit de la donnée secrète sur le bus de données.

La loi de transfert du procédé définit l'ordre dans lequel les données sont transférées de la mémoire morte ROM vers la mémoire vive RAM, c'est-à-dire l'ordre dans lequel les octets de la données secrète transitent sur le bus de données.

Selon un mode de réalisation, le procédé de l'invention utilise une permutation comme loi de transfert, un ou des paramètres de la permutation étant choisi(s) aléatoirement. Le procédé de l'invention comprend les étapes suivantes, conformément à la figure 2 :

E0 : initialisation du procédé : choix des paramètres de la loi de transfert,

E1 : initialisation d'un indice de boucle j = 0 et d'un indice courant X = X0,

E2 : répétition de N fois les étapes suivantes :

ET1 : lecture de l'octet Oct_X de poids X de la donnée à transférer, situé à l'adresse s_X de la mémoire morte ROM, et mémorisation de l'octet lu dans le registre RA de l'unité de commande UC,

ET2 : écriture, à l'adresse d_X de la mémoire vive RAM, de l'octet contenu dans le registre RA,

ET3 : incrémentation de l'indice de boucle j (j = j+1) et variation de l'indice courant X en fonction de l'indice de boucle j.

La loi de transfert du procédé de l'invention définit l'ordre dans lequel les octets de la donnée secrète transitent sur le bus de données DBUS, cet ordre étant défini par les variations de l'indice courant X en fonction de l'indice de boucle j. L'indice courant X peut varier de différentes manières, l'essentiel étant que, au cours de la réalisation de l'étape E2, l'indice courant X prenne une et une seule fois l'ensemble des valeurs entières comprises entre 0 et N-1.

D'une manière générale, le procédé de l'invention propose de réaliser des permutations caractérisées par la loi de transfert suivante :

$$X = (X0 + SENS * PAS * j) \text{ modulo } N,$$

X étant l'indice courant indiquant le poids de l'octet à transférer, j étant l'indice de boucle du procédé variant entre 0 et N-1, PAS, X0 et SENS étant trois paramètres de la loi de permutation. L'indice courant X est mémorisé dans le registre RX de l'unité de commande UC.

Le premier paramètre PAS, compris entre 0 et N-1, définit la différence, modulo N, entre les poids respectifs de deux octets transférés successivement. Par exemple, si les octets Oct_0 et Oct_3 de la donnée secrète, de poids respectifs 0 et 3, transitent successivement sur le bus DBUS, le pas de la permutation est PAS = 3 - 0 = 3.

Le second paramètre X0, compris entre 0 et N-1, définit le poids du premier octet transféré lors de la mise en œuvre du procédé.

Le troisième paramètre SENS prend deux valeurs 1 ou -1, qui indiquent dans quelle direction le procédé parcourt l'ensemble des octets de la donnée à transférer.

Le choix des paramètres de la permutation est important. En effet, au cours de la réalisation de l'étape E2 du procédé, l'indice courant X doit prendre toutes les valeurs entières comprises entre 0 et N-1 lorsque que l'indice de boucle j varie de 0 à N-1.

Dans un premier mode de réalisation de l'invention, le paramètre PAS est choisi aléatoirement et les paramètres X0 et SENS sont constants, mémorisés dans la mémoire morte ROM du circuit programmable. Pour ce mode de réalisation et lors de l'étape d'initialisation du procédé E0, le générateur de nombres aléatoires GA fournit un nombre aléatoire à l'unité de commande UC, lorsqu'un signal de commande CO est reçu. Eventuellement, si le nombre aléatoire est supérieur à N-1, l'unité de commande UC le réduit modulo N pour obtenir un paramètre PAS compris entre 0 et N-1. Enfin, l'unité de commande UC va lire dans la mémoire morte les valeurs du point de départ X0 et du sens de la permutation SENS.

Par exemple, pour le transfert d'une donnée de N = 4 octets, si le générateur GA fournit un nombre PAS = 1 et si X0 = 2 et SENS = 1, la loi de transfert s'écrit "X = (2+j) modulo 4" et les octets de la données seront transférés dans l'ordre suivant : d'abord Oct_2, puis Oct_3, puis Oct_0 puis Oct_1.

Dans un autre exemple, si PAS = 3 (avec X0 = 2 et SENS = 1), la loi de transfert s'écrit "X = (2+3*j) modulo 4" et les octets de la donnée seront transférés dans l'ordre suivant : d'abord Oct_2, puis Oct_1, puis Oct_0, puis Oct_3.

Le paramètre PAS et le nombre N d'octets à transférer doivent être choisis premiers entre eux pour obtenir le transfert de tous les octets de la donnée. Pour cela, le nombre N est de préférence un nombre premier. Dans le cas contraire, il est possible de compléter les octets de poids forts de la donnée par des

"0" afin d'obtenir un nombre N premier d'octets à transférer. Cependant, si le nombre N n'est pas premier, il est également possible d'utiliser une unité de commande comprenant des moyens pour vérifier que le nombre PAS fourni par le générateur GA et le nombre N sont premiers entre eux, et des moyens pour demander éventuellement un nouveau nombre aléatoire PAS au générateur GA.

Dans ce premier mode de réalisation du procédé de l'invention, le nombre PAS, choisi aléatoirement et éventuellement réduit modulo N si nécessaire, peut prendre au maximum N valeurs différentes 0 à N-1, l'ensemble des octets de la donnée secrète peut donc être transféré dans N ordres différents.

Dans un second mode de réalisation de l'invention, le point de départ X0 est choisi aléatoirement et les paramètres PAS et SENS sont constants, mémorisés dans la mémoire morte ROM du circuit programmable CP. Pour ce mode de réalisation et lors de l'étape d'initialisation du procédé E0, le générateur de nombres aléatoires GA fournit un nombre quelconque à l'unité de commande UC, lorsqu'un signal de commande CO est reçu. Eventuellement, si le nombre aléatoire fourni est supérieur à N-1, l'unité de commande UC le réduit modulo N pour obtenir un point de départ X0 compris entre 0 et N-1. Enfin, l'unité de commande UC va lire dans la mémoire morte ROM les valeurs des paramètres PAS et SENS.

Par exemple, pour le transfert d'une donnée de N = 4 octets, si le générateur GA fournit un point de départ X0 = 2 et si PAS = 1 et SENS = -1, la loi de transfert s'écrit "X = (2-j) modulo 4" et les octets de la données seront transférés dans l'ordre suivant : d'abord Oct_2, puis Oct_1, puis Oct_0 puis Oct_3. Dans un autre exemple, si X0 = 3 (avec PAS = 1 et SENS = -1), les octets de la donnée seront transférés dans l'ordre

suivant : d'abord Oct_3, puis Oct_2, puis Oct_1 puis Oct_0.

Pour ce second mode de réalisation, le point de départ X0, choisi aléatoirement et éventuellement réduit modulo N si nécessaire, peut prendre au maximum N valeurs différentes comprises entre 0 et N-1. Ainsi, lors de chaque transfert de la donnée, l'ensemble des octets peut donc être transféré dans N ordres différents.

Dans un troisième mode de réalisation de l'invention, le sens de la permutation SENS est choisi aléatoirement et les paramètres PAS et X0 sont constants, mémorisés dans la mémoire morte ROM du circuit programmable CP. Pour ce mode de réalisation et lors de l'étape d'initialisation du procédé E0, le générateur de nombres aléatoires GA fournit un nombre aléatoire à l'unité de commande UC, lorsqu'un signal de commande CO est reçu. Eventuellement, si le nombre aléatoire fourni est supérieur à 1, l'unité de commande UC le réduit modulo 2 pour obtenir un nombre aléatoire égal à 0 ou 1. Puis, si le nombre aléatoire est égal à "0" alors l'unité de commande choisit SENS = -1 et inversement, si le nombre aléatoire est égal à 1, l'unité de commande choisit SENS = 1. Au cours de l'étape E0, l'unité de commande UC va ensuite lire dans la mémoire morte ROM les valeurs du paramètre PAS et du point de départ de la permutation X0.

Par exemple, pour le transfert d'une donnée de N = 4 octets, si le générateur GA fournit un sens de permutation SENS = 1 et si PAS = 1 et X0 = 0, les octets de la données seront transférés dans l'ordre suivant : d'abord Oct_0, puis Oct_1, puis Oct_2 puis Oct_3. Dans un autre exemple, si SENS = -1 (avec PAS = 1 et X0 = 0), les octets de la donnée seront transférés dans l'ordre suivant : d'abord Oct_0, puis Oct_3, puis Oct_2 puis Oct_1.

Pour ce troisième mode de réalisation, le paramètre SENS, choisi aléatoirement et éventuellement réduit

modulo 2 si nécessaire, peut prendre au maximum 2 valeurs différentes 0 et 1. Ce troisième mode de réalisation est donc moins performant dans la mesure où le nombre de combinaisons différentes de l'ensemble des octets de la donnée à transférer est limité à 2 : la donnée peut donc être assez facile à trouver.

Il est également possible de combiner les premier et/ou second et/ou troisième modes de réalisation de l'invention pour obtenir un procédé de transfert plus sûr. Par exemple, Dans un quatrième mode de réalisation de l'invention, les trois paramètres de la loi de permutation, PAS, X0 et SENS sont choisis aléatoirement.

Pour ce mode de réalisation et lors de l'étape d'initialisation du procédé E0, le générateur de nombres aléatoires GA fournit d'abord un premier nombre aléatoire à l'unité de commande UC, lorsqu'un premier signal de commande CO_1 est reçu. Eventuellement, si le premier nombre aléatoire est supérieur à N-1, l'unité de commande UC le réduit modulo N pour obtenir un paramètre PAS compris entre 0 et N-1.

Le générateur GA fournit ensuite un second nombre aléatoire à l'unité de commande, lorsqu'un second signal de commande CO_2 est reçu. Eventuellement, si le second nombre aléatoire est supérieur à N-1, l'unité de commande UC le réduit modulo N pour obtenir un point de départ X0 compris entre 0 et N-1.

Puis, lorsqu'un troisième signal de commande CO_3 est reçu, le générateur GA fournit un troisième nombre aléatoire qui est éventuellement réduit modulo 2 par l'unité de commande s'il est supérieur à 1. Enfin, l'unité de commande choisit SENS = -1 si le troisième nombre aléatoire est égal à 0, et SENS = 1 si le troisième nombre aléatoire est égal à 1.

Ce quatrième mode de réalisation est particulièrement intéressant. En effet, puisque tous les

paramètres de la permutation PAS, X0 et SENS sont choisis aléatoirement, il existe p*N*2 combinaisons possibles des octets d'une même donnée, p étant le nombre de valeurs possibles pour le paramètre PAS sachant que PAS et N doivent être premiers entre eux. Si de plus, le nombre N est premier, il existe un nombre maximal 2*N*N de combinaisons possibles des octets d'une même donnée, il est donc plus difficile de trouver la bonne valeur de la donnée transférée.

Bien sûr, toute autre combinaison possible des premier, second et troisième modes de réalisation de l'invention est possible. Par exemple, il est possible de choisir aléatoirement le paramètre PAS et le point de départ X0 et de fixer la valeur de SENS à 1 ou -1.

Un avantage de l'invention est de rendre inopérante la technique d'espionnage d'analyse de courant. En effet, si K mesures de courant sont effectuées lors de K transferts de la même donnée sur le bus DBUS et si une moyenne de ces K mesures est effectuée pour éliminer le bruit de la mesure, le résultat obtenu sera une donnée ayant 8*N bits identiques égaux à la valeur moyenne des 8*N bits de la donnée réelle.

Un autre avantage de l'invention est de proposer un procédé de transfert de données qui peut être utilisé en parallèle avec d'autres procédés de protection de données, sans perturber le fonctionnement de ces derniers. Par exemple, dans la description ci-dessus, les adresses s_0 à s_{N-1} et d_0 à d_{N-1} ont été supposées consécutives. Néanmoins, il serait tout-à-fait possible de transférer des données dont les octets sont éparpillés dans la mémoire ROM.

REVENDICATIONS

1. Procédé de transfert sécurisé de données dans un circuit programmable (CP) comprenant une unité de commande (UC), une mémoire morte (ROM) comprenant des données à transférer, une mémoire inscriptible (RAM) et un bus de données (DBUS) connecté entre la mémoire morte (ROM) et la mémoire inscriptible (RAM), le bus de données (DBUS) étant commandé par l'unité de commande (UC),

le procédé de transfert étant caractérisé en ce qu'une donnée secrète à transférer de N octets transite octet par octet sur le bus de données (DBUS), chaque octet transitant une seule fois sur le bus de données,

et en ce que les octets sont transférés selon une loi de transfert ayant au moins un paramètre choisi de manière aléatoire par l'unité de commande (UC) avant chaque transfert de la donnée secrète.

2. Procédé selon la revendication 1, caractérisé en ce que la loi de transfert est une permutation des éléments de l'ensemble des N octets de la donnée secrète à transférer.

3. Procédé selon la revendication 2, caractérisé en ce que la permutation est définie par la relation

$$X = (X0 + SENS * PAS * j) \text{ modulo } N,$$

où un premier paramètre (PAS), compris entre 0 et N-1, définit le pas de la permutation,

où un second paramètre (SENS), prenant deux valeurs 1 ou -1, définit le sens de parcours de l'ensemble des N octets de la donnée secrète,

où un troisième paramètre (X0), compris entre 0 et N-1, définit le point de départ de la permutation,

et où un indice courant (X), obtenu à partir des premier à troisième paramètres (PAS, SENS, X0) et d'un indice de boucle (j) variant entre 0 et N-1, indique le poids d'un octet de la donnée secrète à transférer.

4. Procédé selon la revendication 3, caractérisé en

ce que le premier paramètre (PAS) est choisi aléatoirement par l'unité de commande (UC), avant chaque transfert de la donnée secrète.

5. Procédé selon l'une des revendications 3 ou 4, caractérisé en ce que le second paramètre (SENS) est choisi aléatoirement par l'unité de commande (UC), avant chaque transfert de la donnée secrète.

6. Procédé selon l'une des revendications 3 à 5, caractérisé en ce que le troisième paramètre (X0) est choisi aléatoirement par l'unité de commande (UC), avant chaque transfert de la donnée secrète.

7. Procédé selon l'une des revendications 3 à 6, caractérisé en ce que le premier (PAS) et le troisième paramètre (X0) sont choisis aléatoirement par l'unité de commande (UC), avant chaque transfert de la donnée secrète.

8. Procédé selon l'une des revendications 3 à 7, caractérisé en ce que le premier paramètre (PAS) de la permutation et le nombre N sont premiers entre eux.

9. Procédé selon l'une des revendications 3 à 8, caractérisé en ce que le nombre N est un nombre entier premier et en ce que le premier paramètre (PAS) de la permutation est un nombre entier compris entre 1 et N-1.

10. Procédé selon l'une des revendications 3 à 9, caractérisé en ce qu'il comprend les étapes suivantes :

E0: Initialisation du procédé et choix des premier à troisième paramètres (PAS, SENS, X0), l'un au moins des premier à troisième paramètres étant choisi aléatoirement par l'unité de commande (UC), les premier à troisième paramètres (PAS, SENS, X0) étant mémorisés dans un premier registre (RX) de l'unité de commande (UC),

E1 : Initialisation d'un indice de boucle (j) et d'un indice courant (X),

E2 : Répétition N fois des étapes suivantes :

ET1 : lecture, dans la mémoire morte (ROM) d'un octet de la donnée à transférer, le poids de l'octet lu

étant égal à l'indice courant (X), et mémorisation de l'octet lu dans un second registre (RA) de l'unité de commande,

ET2 : écriture dans la mémoire vive (RAM), de l'octet contenu dans le second registre (RA),

ET3 : incrémentation de l'indice de boucle (j) et variation de l'indice courant (X).

11. Circuit programmable (CP) comprenant une unité de commande (UC), une mémoire morte (ROM) comprenant des données à transférer, une mémoire inscriptible (RAM) et un bus de données (DBUS) connecté entre la mémoire morte (ROM) et la mémoire inscriptible (RAM), le bus de données (DBUS) étant commandé par l'unité de commande (UC),

le circuit programmable (CP) étant caractérisé en ce qu'il comporte en outre un générateur de nombres aléatoires (GA) pour fournir au moins un paramètre d'une loi de transfert de données utilisée pour transférer une donnée secrète de N octets de la mémoire morte (ROM) vers la mémoire vive (RAM), les octets de la donnée secrète à transférer transitant octet par octet sur le bus de données (DBUS), chaque octet transitant une seule fois sur le bus de données (DBUS), l'au moins un paramètre étant différent à chaque transfert de la donnée secrète.

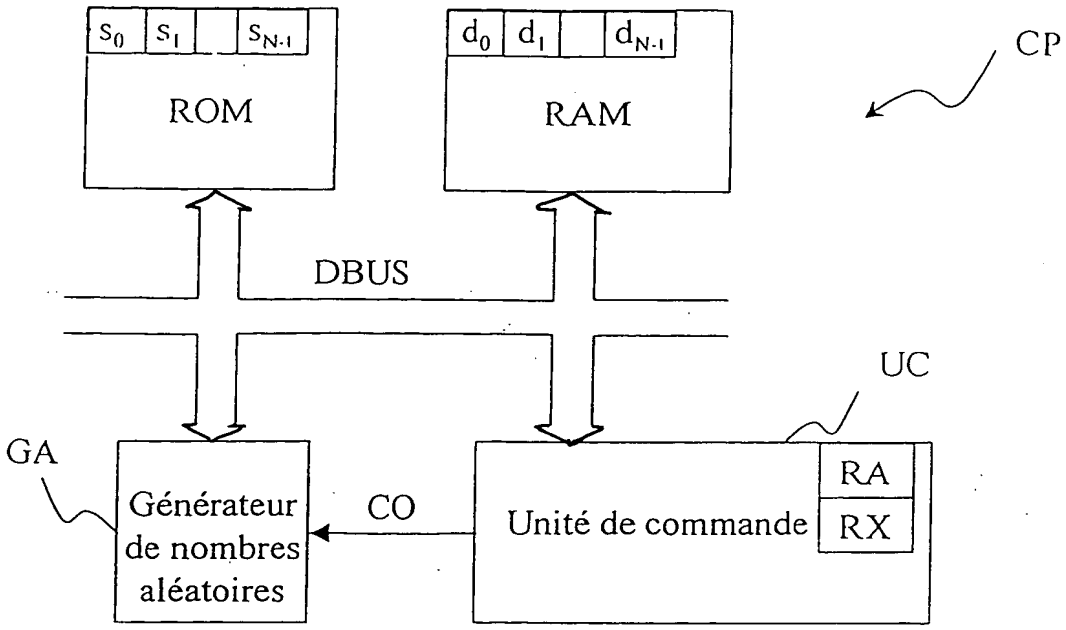

Fig. 1

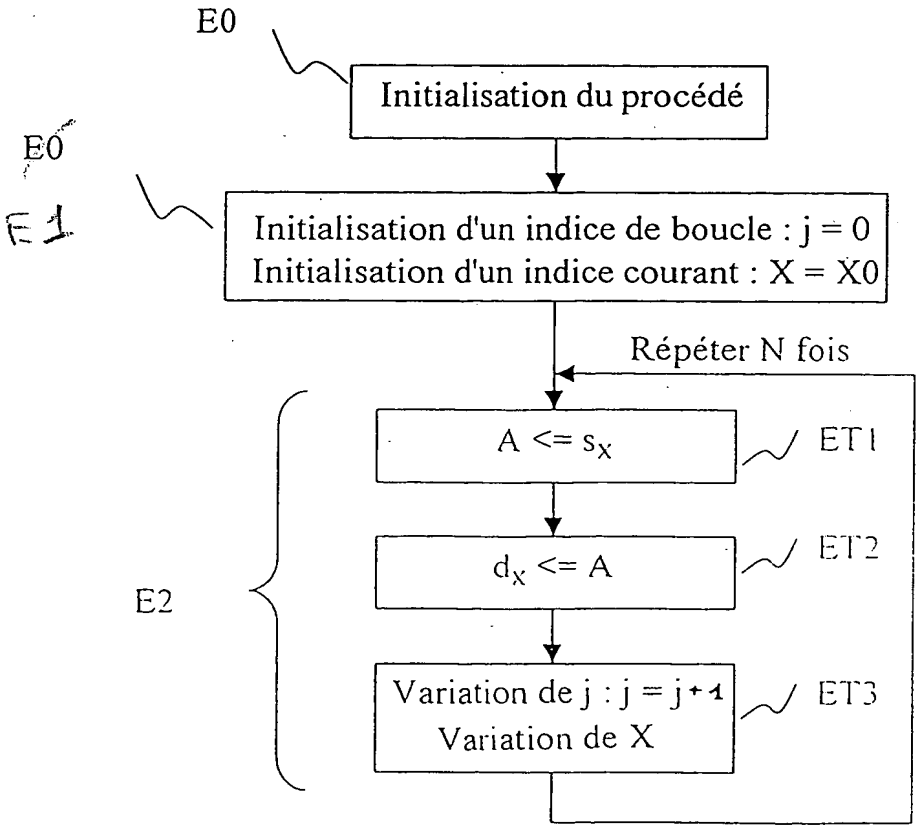

Fig. 2

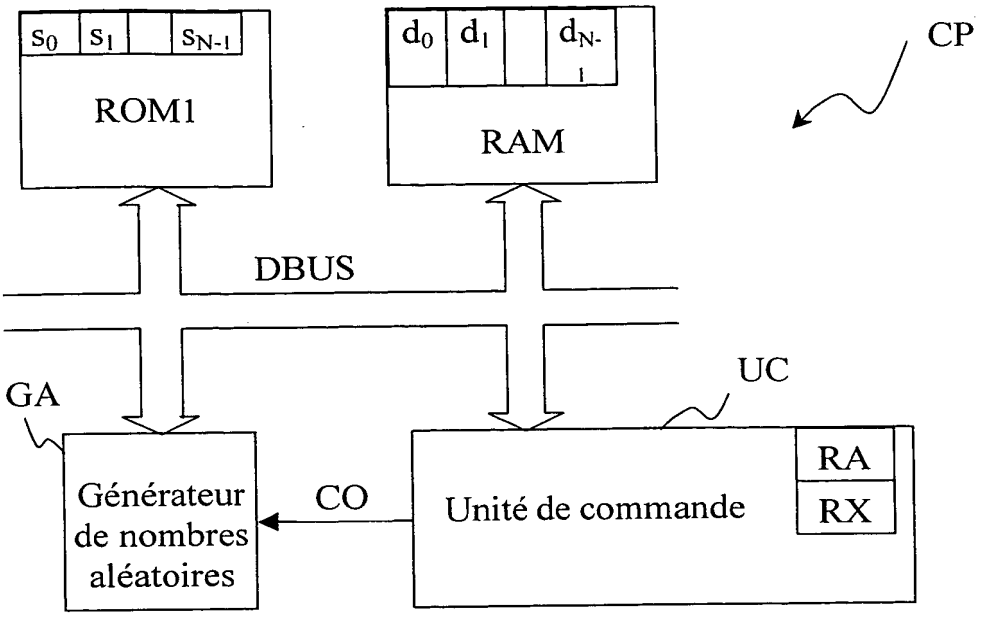

Fig. 1

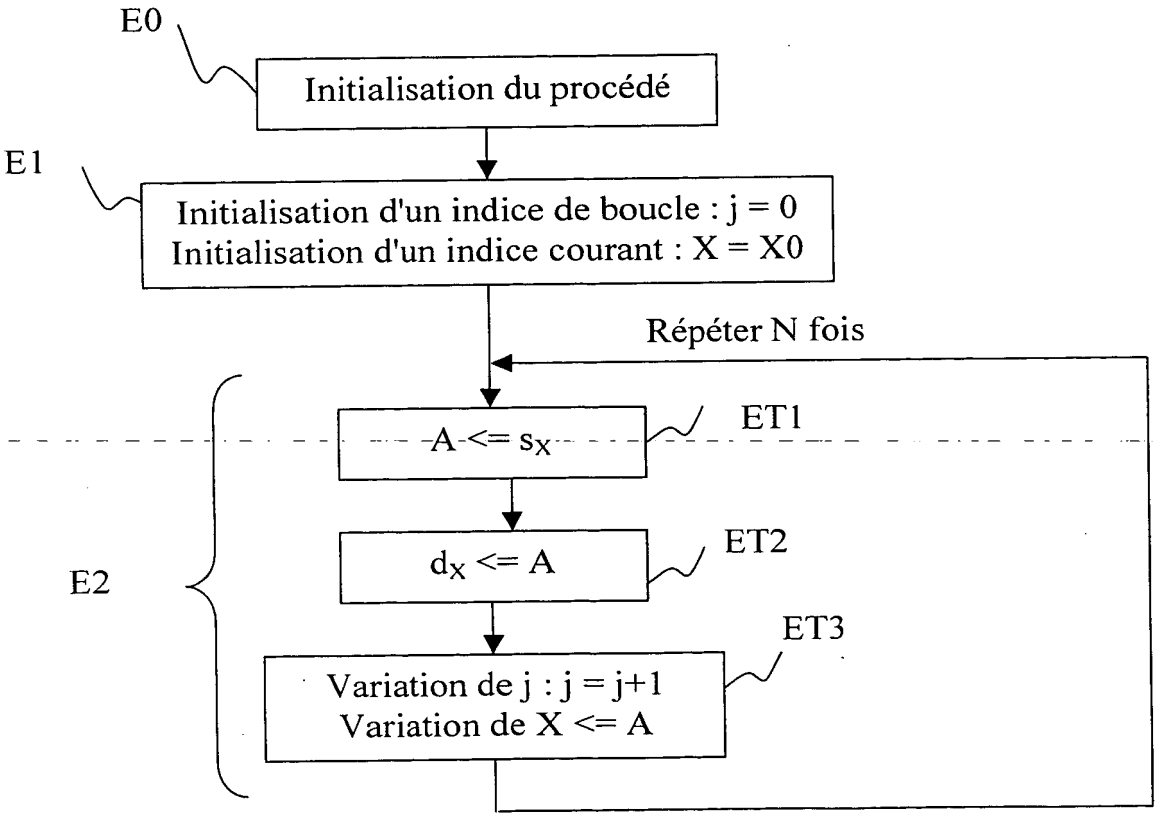

Fig. 2